CLAIMS

1. A method of processing network security protocol data packets, comprising:

providing a cryptography processing architecture on a chip;

passing non-pre-padded network security protocol data for both authentication and cryptography operations from a source to said chip;

conducting, in hardware, authentication and encryption, operations on the network security protocol data; and

passing the cryto-processed network security protocol data from said chip to said source;

wherein said non-pre-padded network security protocol data is passed between said chip and said source in a single pass.

2. The method of claim 1, wherein said network security protocol is SSL (v3).

3. The method of claim 1, wherein said network security protocol is TLS.

4. The method of claim 1, further comprising simultaneously with conducting the cryptography operations on the data, pre-loading network security protocol data from a second non-pre-padded network security protocol packet onto the chip.

5. The method of claim 4, further comprising simultaneously with conducting the encryption operations on the data, conducting, in hardware, authentication operations

on the network security protocol data from the second network security protocol packet.

6. The method of claim 1, wherein said conducting, in hardware, authentication and encryption operations on the non-pre-padded network security protocol data comprises conducting padding and alignment operations on the chip.

7. The method of claim 6, wherein said calculation of a pad length for padding operations is conducted by a pad engine component of the chip architecture.

8. The method of claim 1, wherein said conducting, in hardware, authentication and encryption operations on the network security protocol data comprises feeding back a MAC value calculated during authentication operations for processing in the encryption operations.

9. The method of claim 1, wherein said encryption operations further include decryption operations.

10. The method of claim 9, wherein conducting, in hardware, authentication and decryption operations on the network security protocol data comprises feeding back decrypted data for processing in the authentication operations.

11. A cryptography accelerator chip architecture, comprising:

an authentication component;

an encryption component; and

a pad engine computing and outputting pad length and pad to said encryption component.

12. The cryptography accelerator chip architecture of claim 11, wherein said architecture is configured to process non-pre-padded network security protocol packets.

13. The cryptography accelerator chip architecture of claim 11, wherein said chip resides on an expansion card.

14. The cryptography accelerator chip architecture of claim 11, wherein said authentication component comprises an alignment block, an authentication data input buffer, and an authentication engine.

15. The cryptography accelerator chip architecture of claim 11, wherein said encryption component comprises an alignment block, an encryption data input buffer, and an encryption engine.

16. The cryptography accelerator chip architecture of claim 6, wherein said architecture is configured to process SSL data.

17. The cryptography accelerator chip architecture of claim 6, wherein said architecture is configured to process TLS data.

18. An electronic commerce computer network system, comprising:

a front end data source;

a PCI bus connecting said front end data source to a cryptography accelerator chip architecture, said architecture having,

an encryption component;

an authentication component, and

a pad engine computing and outputting pad length and pad to said encryption component.

19. The system of claim 18, wherein said front end data source comprises:

one or more network interfaces;

a processor connected with said interfaces;

a memory connected with said processor; and

a bridge and memory controller connected with said processor and memory.

20. The system of claim 18, wherein said chip resides on an expansion card.

21. The system of claim 18, wherein said architecture is configured to process network security protocol packets.

22. The system of claim 18, wherein said authentication component comprises an alignment block, an authentication data input buffer, and an authentication engine.

23. The system of claim 18, wherein said encryption component comprises an alignment block, an encryption data input buffer, and an encryption engine.

75 24. The system of claim 18, wherein said network security protocol is SSL (v3).

76 25. The system of claim 18, wherein said network security protocol is TLS.

77